REMARKS/ARGUMENTS

The Office Action has been carefully considered. It is respectfully submitted that the issues raised are traversed, being hereinafter addressed with reference to the relevant headings appearing in the Detailed Action section of the Office Action.

35 USC § 102

At pages 2 - 4 of the Office Action, the Examiner rejects claims 1, 2, 4, 6, 7 and 11 under 35 USC § 102(e) as being anticipated by US Patent No. 5,923,759 (Lee). The applicant asserts that the Examiner has incorrectly raised Lee as anticipating the claims of the present invention.

Referring to claim 1 of the present application, the step of "comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first key or the second key" is not disclosed in Lee. This is an important feature of the present claims and Lee teaches a very different comparison.

Referring to column 6, lines 37 - 52 (also cited by the Examiner), Lee clearly teaches "processor 122 decrypts the number based upon the same algorithm and an identifying key stored in memory 126". It is one of the major advantages of the presently claimed invention that a key is not revealed during the authentication process. Referring to Fig. 3 of the present application, the secret key of chip A 20 or the secret key of chip T 23 are not revealed to system 21 when comparing $S_{KT}[R]$ 34 and $S_{KA}[R]$ 35. This is clearly reflected in claim 1 of the present application that the first encrypted outcome and the second encrypted outcome are compared without knowledge of the first key or the second key.

This is clearly not the situation in Lee as "the encryption used to encrypt data received from smart cards are stored in secure data memory 126 and are preferably only accessible via processor 122" (column 4, lines 16 - 18). Also, in Lee, "processor 122 can request a key from memory 126" (column 4, line 21). This is obviously not the validation protocol claimed in present claim 1 as clearly processor 122 has knowledge of an encryption key

stored in memory 126. This is an important difference between the present invention, as claimed in claim 1, and Lee. Thus, Lee does not anticipate present claim 1.

Still furthermore, Lee at column 6, lines 46 - 53 discusses comparison only between the original random number and the encrypted random number, and if they are determined to be the same the card is authentic. Again, this highlights an important difference between the invention claimed in claim 1 and Lee. In present claim 1 the comparison is between "the first encrypted outcome and the second encrypted outcome", not the generated random number. Advantageously, this allows the present invention to test whether an untrusted chip is valid by preparing encrypted responses without having to comprehend or decrypt those encrypted responses.

Lee teaches a markedly different situation whereby processor 126 decrypts the number received from the card using an identifying key stored in memory 126 and then compares the original random number and the decrypted random number. This is not what is claimed in present claim 1 and for this further reason claim 1 is not anticipated by Lee.

Independent claim 6 is to a validation system that includes "comparison means to compare the first encrypted outcome and the second encrypted outcome without knowledge of the first key and the second key. Hence, independent claim 6 is also not anticipated by Lee for at least the reasons presented above.

Likewise, dependent claims 2 - 5 and 7 - 12, that depend from independent claim 1 and 6 respectively, are not anticipated by Lee.

35 USC § 103

As the applicant submits that the anticipation rejection in light of Lee has been overcome and Abraham *et al.* (US Patent No. 4,799,061) does not teach or suggest "comparing the first encrypted outcome and the second encrypted outcome, without knowledge of the first key or the second key" as previously demonstrated in earlier responses, the obviousness rejection is also traversed.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC § 102 and 35 USC § 103. The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under Examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

Applicant:

PAUL LAPSTUN

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9555 7762